What is claimed is:

1. A FIPS-compliant QKD-based encryption system, comprising:

a FIPS-complaint VPN having first and second VPN stations;

a classical encryption system having first and second operatively connected encryption/decryption (e/d) processors operatively connected to the first and second VPN stations, respectively;

a QKD system having first and second operatively connected QKD stations respectively operatively connected to the first and second e/d processors, the QKD system being adapted to exchange a quantum key between the first and second QKD stations and provide the quantum key to the first and second e/d processors; and

wherein the classical encryption system is adapted to receive a VPN signal from the VPN and encrypt the VPN signal using the quantum key.

2. The system of claim 1, further including first and second transmitting/receiving stations operatively connected to the first and second VPN stations, respectively, wherein the first and second transmitting/receiving stations are adapted to transmit and/or receive plaintext signals to and from the respective first and second VPN stations.

3. The system of claim 1, wherein the first and second e/d processors are connected by an Ethernet section.

4. The system of claim 1, wherein the first and second VPN stations are computers.

5. The system of claim 1, wherein the e/d processors each include a quantum key storage device for storing the quantum key provided by the QKD system.

6. A FIPS-complaint QKD-based encryption system, comprising:

a FIPS-compliant VPN layer;

a classical encryption layer operatively connected to the FIPS-compliant VPN layer;

a QKD layer operatively connected to the classical encryption layer; and

wherein the QKD layer provides a quantum key to the classical encryption layer so that the classical encryption layer is capable of encrypting information from the FIPS-compliant VPN layer using the quantum key.

7. The system of claim 6, wherein the classical encryption layer includes first and second encryption/decryption (e/d) processors, and wherein:

the QKD layer includes first and second QKD stations respectively operatively coupled to the first and second e/d processors and adapted to symmetrically distribution the quantum key to the first and second e/d processors.

8. A FIPS-compliant encryption system comprising:

first and second transmitters/receivers operatively connected through a FIPS-compliant VPN;

a classical encryption system operatively connected to the FIPS-compliant VPN and to a QKD system; and

wherein the QKD system provides a quantum key to the classical encryption system, which then uses the quantum key to encrypt and decrypt a plaintext signal input from one of the first and second transmitters/receivers.

9. The system of claim 8, wherein the classical encryption system is FIPS-compliant.

10. A method of forming a FIPS-compliant QKD encryption system using a FIPS-compliant VPN, the method comprising:

forming a classical encryption link by operatively connecting first and second operatively connected encryption/decryption (e/d) processors to respective first and second VPN stations of the FIPS-compliant VPN; and

operatively connecting first and second operatively connected QKD stations of a QKD system to the first and second e/d processors, respectively, the first and second QKD stations capable of exchanging a quantum key and providing the quantum key to the first and second e/d processors.

11. The method of claim 10, including operatively connecting first and second transmitting/receiving stations to the first and second VPN stations, respectively, wherein the first and second transmitting/receiving stations are adapted to transmit and/or receive plaintext signals.

12. The method of claim 10, including operatively connecting the first and second e/d processors by an Ethernet section.

13. A method of transmitting an encrypted signal between first and second transmitting/receiving stations, comprising:

sending a first plaintext signal from the first transmitting/receiving station to a first VPN station of a FIPS-compliant VPN;

converting the first plaintext signal to a first VPN signal at the first VPN station;

providing the first VPN signal to a first encryption/decryption (e/d) processor of a classical encryption system also having a second e/d processor;

exchanging a quantum key between first and second QKD stations in a QKD system and providing the quantum key to the first and second e/d processors;

forming an encrypted VPN signal from the first VPN signal at the first e/d processor using the quantum key provided to the first e/d processor;

forming a decrypted VPN signal from the encrypted VPN signal at the second e/d using the quantum key provided to the second e/d processor;

forming second plaintext signal from the decrypted VPN signal at a second VPN station in the VPN; and

receiving the second plaintext signal at the second transmitting/receiving station.

14. A method of forming a FIPS-compliant encryption system that utilizes quantum key distribution (QKD), comprising:

providing a FIPS-complaint VPN;

forming a classical encryption link within the FIPS-compliant VPN; and

providing a quantum key to the classical encryption link so that the classical encryption link is capable of encrypting information input to the FIPS-compliant VPN using the quantum key.

15. The method of claim 14, wherein the classical encryption link includes first and second encryption/decryption (e/d) processors, and further including:

interfacing the first and second e/d processors with respective first and second QKD stations; and

performing symmetric quantum key distribution between the first and second QKD stations and the first and second e/d processors.

16. The method of claim 14, including forming the classical encryption link with a FIPS-compliant classical encryption link.